European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2022.01.4

SLCMC 2021
International conference «State and law in the context of modern challenges»

CYBER-LIBEL: PROVING AND QUALIFICATION CHALLENGES

Evelina G. Aniskina (a)*, Natalia E. Mullakhmetova (b), Anna A. Magankova (c)
*Corresponding author

(a) Saratov State Law Academy. Smolensk branch, 3, Udarnikov St., Smolensk, Russia, evashkredova@mail.ru,
(b) Saratov State Law Academy. Smolensk branch, 3, Udarnikov St., Smolensk, Russia, nati16011978@mail.ru,
(c) Saratov State Law Academy. Smolensk branch, 3, Udarnikov St., Smolensk, Russia, aasivolova@rambler.ru

Abstract

The article addresses the problem of the information and telecommunications-related crimes growth worldwide. In particular, it points to the latent, transnational and remote nature of such crimes. The authors refer to the criminal law aspects of cyber-libel, as well as on the issues of proving its corpus delicti. The authors define the time when the defamation stops in view of the introduction of a new ground of libel in art. 128.1 of the Criminal Code of the Russian Federation – "committed publicly using information and telecommunications networks, including the Internet". The correct determination of this point affects the manner of application of limitation and amnesty statutes. The authors recognize the continuing nature of defamation through the Internet with intent to spread false information to an unspecified number of people for an indefinite period of time. The moment of the cessation in this case should be determined based on the fact that there are two such moments in a continuing crime – de facto and de jure. The authors note that libel on the above ground is now a public prosecution case, the burden of proof is therefore on the person conducting the investigation. In order to optimize the investigation of crimes committed with the use of the Internet, including defamation, it is necessary to legislate the procedure for seizure of information posted on the Internet in order to give it an evidentiary value, as well as to involve a specialist to this procedural action.

Keywords: Evidence, information and telecommunication space, internet, Libel

https://doi.org/10.15405/epsbs.2022.01.4
Corresponding Author: Evelina G. Aniskina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The official statistics of the Ministry of Internal Affairs of the Russian Federation show that the number of crimes committed using information and telecommunication technologies is increasing rapidly in recent years. In 2020 alone, 510,400 attacks were detected, an increase of 73.4per cent over the previous year, this accounts for 25 per cent of the total number of crimes. The particular maliciousness of the new method in the commission of a number of crimes – "using a telecommunications network of information, including the Internet" – lies in the lightning-fast and large-scale spread of information, which is due to the diversity of resources used on the Internet, including electronic media, websites of executive authorities, social networks, etc., as well as an unlimited number of users. Moreover, it is the information and telecommunication environment that remains under weak control of the state compared to the real environment, which is exacerbated by the problem of identifying perpetrators of crimes on the Internet, including libel (due to the anonymity and ease of defamation on the Internet), the difficulties of proof in criminal cases. Collecting, checking and evaluating evidence during the investigation of libel on the Internet requires the use of special knowledge not only in linguistics, but also in information and telecommunications technology. The problem of prosecuting individuals is noteworthy due to the fact that the crime can be committed remotely. The location of the perpetrator of a socially dangerous and criminally offensive act, the location of the computer used to spread information, and the residence of the victim may not coincide, that is, given those locations, crimes can be both domestic and transnational in nature, including cases where the co-perpetrators are citizens of different states. Thus, the commission of crimes using the Internet, including defamation, is characterized by latency, transnationality and remoteness. Western scholars also drew attention to this problem more than twenty years ago (Metchik, 1997). Also, it is important to consider that the optimal criminal law regulation of liability for libel, including on the Internet, presupposes ensuring a reasonable balance between the constitutional right to freedom of thought and speech and the right to protection of honor and dignity. In the scientific community, defamation on the Internet refers to cybercrimes, since here the computer network is used as a means of committing a crime. Scientists are widely discussing the problems of liability for sending (repost) libelous information, as well as differentiating liability for libel, depending on the consequences for the victim (Li & Qin, 2018).

2. Problem Statement

Today, the Internet has become a public platform for the exchange of information, the reliability of which is often highly questionable. If in the last century the publication of materials in the media was not available to everyone, it assumed censorship, then now any person, even without experience in the field of journalism, any specialized education, can make various photo-, video images, texts available to the public. Today this problem is increasingly being raised in the domestic and foreign scientific literature (Lewis, 2015). Representatives of the criminal world are also actively conquering the Internet space, invent all-new ways of committing crimes (including libel, fraud, illegal circulation of narcotic drugs and psychotropic substances). The growth of so-called cybercrime has led to the emergence of new scientific directions related to the study of the patterns of committing criminal attacks on the Internet, the problems

https://doi.org/10.15405/epsbs.2022.01.4
Corresponding Author: Evelina G. Aniskina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

of their detection, prevention, and investigation. In recent publications, Internet security problems are studied in various aspects: criminal law, criminology, criminal procedure, the positive experience of foreign countries is analyzed; proposals are developed to improve legal regulation and practice in this area (Shukan et al., 2019).

The above mentioned information explains the state response, through its legislation, to the new challenges of our time. This is reflected in the reform of criminal legislation, namely the differentiation of criminal responsibility by including a number of qualifying attributes to formulations of a new method and means of committing a crime – "using information and telecommunications networks, including the Internet".

Analysis of the Criminal Code of the RF shows that 17 articles provide the qualifying criterion for aggravation of the penalty as compared with the first parts. Most often these are acts involving the dissemination of information (e.g. libel; cruelty to animals (in terms of public demonstration); inducing or involving a person in any destructive (e.g. incitement to suicide; involving a minor in committing acts endangering the life of a minor), socially dangerous (e.g. inducement to use narcotic drugs, psychotropic substances or their analogues) or criminal activity (e.g. public incitement of terrorist activities; publicly broadcast appeals for actions violating the territorial integrity of the Russian Federation), as well as promotion of prohibited items (e.g. illicit production, sale or trafficking of narcotic drugs, psychotropic substances or their analogues, as well as illegal sale or transfer of plants containing narcotic drugs or psychotropic substances or their parts containing narcotic drugs or psychotropic substances; illegal production and trafficking of pornographic materials or items). The positive trend towards increasing criminalization of the use of the Internet in a number of articles of the Criminal Code is marred by two shortcomings. Firstly, there is the absence of this element in other corpus delicti also possibly related to the informational influence of the Internet, which is unjustified (in particular, indecent assault; human trafficking; enticement into prostitution; public incitement to a war of aggression; the rehabilitation of Nazism, etc.).

However, the last two corpus delicti include a specific aggravating circumstance, "using mass media", but no mention of the Internet. Secondly, there is the use of different terminology by the legislature for the same method and means (using: information and telecommunication networks (including the Internet) – in most articles; information and telecommunication networks, including the Internet (Article 128.1, Article 238.1, Article 280), information and telecommunication networks (Article 137); electronic or information telecommunication networks, including the Internet (Article 205.2; 258.1); electronic or information and telecommunication networks (including the Internet) (Article 228.1); mass media, including information and telecommunication networks, (including the "Internet" network) (Articles 242, 242.1). Introduction in accordance with the Federal Law of 30.12.2020 № 538-FL "On Amendments to Article 128.1 of the Criminal Code of the Russian Federation" of the criterion "committed publicly with the use of information and telecommunications networks, including the Internet" in relation to defamation has necessitated the scientific understanding of this novelty, including the determination of the moment of the offense completion.

Criminal procedure and forensic science have not developed standard approaches to proving the use of on-line information including on the facts of defamation. When investigating libel committed in

https://doi.org/10.15405/epsbs.2022.01.4
Corresponding Author: Evelina G. Aniskina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

the virtual space, it becomes necessary to use information posted on social networks and websites to prove it. In the context of digitalization of the life of modern society, new approaches to the implementation of evidence are required. Information fixed on paper can no longer remain the only admissible in criminal proceedings. There is a need to improve the procedural regulation of the evidence collection as well as the development on this basis of private forensic investigation techniques for cyber-crimes.

3. Research Questions

The subject of the study is the issues of qualification of cyber-libel, namely the determination of the moment of cessation of defamation committed through the Internet space.

Furthermore, the authors considered the problematic aspects of proving the cyber defamation, including the collection of information posted on-line with the use of special skills.

4. Purpose of the Study

The purpose of the research is to develop a standard approach for qualifying and proving cyber-libel cases necessary for investigative and judicial authorities, including foreign countries, as well as to substantiate the need to regulate the procedural order for obtaining on-line posted information to be used as evidence.

5. Research Methods

The primary research methods of the research were dogmatic, historical and comparative. Expert interviews with criminal law scholars, judges and lawyers were conducted to address qualification problems in the application of libel legislation, as well as interviewing law enforcement officials on the evidentiary issues of using the information posted on the Internet, including cases of defamation.

6. Findings

The main problem of cyber-libel qualification is the determining the moment of the completion of the crime in question and hence the peculiarities of the application of the statute of limitations and amnesty. The answer to this question is connected to the possibility of recognizing libel as a continuing crime. It seems that libel may be a complex – a continuing crime when there is the intent to do so, for example, if it is an intent to disseminate information through the Internet on a particular site; long-time on-line demonstration of a video with false information.

The above actions are characterized by the continuous implementation of the corpus delicti through the continuous violation of the established prohibition (act of commission), which is the main feature of a continuing crime. With regard to Russian judicial practice, even within a region, some judicial acts (See Appeal Decision No. 10-24/2015 of December 1, 2015 on case No. 10-24/2015 Novokuibyshevsk City Court of Samara region) recognize libel as a continuing crime; others, on the

https://doi.org/10.15405/epsbs.2022.01.4
Corresponding Author: Evelina G. Aniskina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

contrary, the opposite was noted (Decision of August 1, 2016 on case No. 1-61/2016 of the justice of the peace of judicial sub-district No. 69 of Novokuibyshevsk judicial district, Samara region). Our expert survey showed that the majority of scholars, judges and lawyers still do not recognize the continuing nature of libel.

Thus, when asked: "Name the moment of the end of libel in the form of defamation of knowingly false information through the Internet on a certain site, if it was not updated in the future?" 93.3per cent of judges and 84.2 per cent of lawyers answered "the moment of the first publication of information (libel) on the Internet"; and only 6.7 per cent of judges and 15.8 per cent of lawyers answered "the moment when distribution of false information is stopped, for example, the elimination of information on the Internet or apprehension of a criminal"; the opinion of scientists does not differ notably: 83.9 per cent answered "the moment of the first publication of information (libel) on the Internet"; 16.1 per cent answered "the moment when distribution of false information is stopped". It is also worth noting separately the opinion of Russian scientists that only in cases where the perpetrator has created a certain information resource (website, questionnaire, etc.) where information is updated or new materials are added, the crime should be characterized as having a long-term nature from the first publication to the last change (Shirkin & Erashova, 2019).

Internet defamation cases have been publicly investigated since 2021, so the burden of proof is on the investigator, not on the private prosecutor, as it may have been previously. The process of obtaining on-line information is not sufficiently regulated in the CPC RF, there are only articles referred to the seizure of electronic media (Article 164.1 of the CPC RF) but not the information itself. There is also no definition of electronic evidence in the law, although definitions have been developed in theory and even a new scientific interdisciplinary in nature branch is elaborated – the theory of electronic evidence (Vekhov, 2016). But not all scientists agree that electronic evidence should be introduced into the Criminal Procedure Code of the Russian Federation as a new type of evidence since the use of the latter in criminal proceedings is possible within the framework of the existing list of evidence: information in electronic form can be considered as material evidence or as other documents.

The main problem is that the participant in the process, submitting electronic evidentiary information, must justify its integrity and invariability, i.e. authenticity (Pastukhov, 2019). Practice provides examples of establishing the very fact of defamatory information dissemination in libel cases using printed screenshots of pages from the Internet (the admissibility of using such printouts as evidence in court is indicated, for example, in paragraph 55 of the Resolution of the Supreme Court of the RF of 23.04.2019 № 10 "On Application of Part Four of the Civil Code of the Russian Federation"). However, it is widespread practice of using notaries to provide evidence and reporting to law enforcement bodies during the crime report verification.

The most difficult evidentiary issue is the identification of the subjective side of the crime (intent and motive for distribution). As it is noted by 67 per cent of the lawyers surveyed, the most commonly used evidence is the testimony of witnesses, inspection reports of objects and documents, including Internet pages of websites where defamatory information is posted (or was posted), and expert opinion. There is also a procedural regime for the use of electronic media, but their very definition is not established.

7. Conclusion

The authors consider cyber-libel to be of a continuing nature when there is the intent to spread false information to an unspecified number of people for an indefinite period of time. The question about the moment of cessation in this case is resolved in view of the fact that there are two such moments in a continuing crime – de facto and de jure.

The factual moment of the end of libel is the moment when the dissemination of false information is stopped, for example, the elimination of on-line information. Investigation of cyber-libel includes not well-developed legislative and scientific investigative actions as interrogation and examination, but also the appointment of linguistic expertise to establish the defamatory nature of the information disseminated, as well as actions aimed at seizure of electronic information.

To ensure the evidentiary basis of cyber-libel cases, more precise legislation was needed to regulate the procedure for seizure of information from sites, along with the necessity of definition by the Criminal Procedural Code of the Russian Federation of the electronic evidence concept, making the participation of specialists mandatory. In this case, the list of evidence set out in Art. 74 of the Code of Criminal Procedure of the Russian Federation, may remain unchanged, you can simply fix the concept of proof that information can also be in electronic form. Electronic evidence should be assessed according to general rules, that is, from the standpoint of relevance, admissibility, reliability.

Acknowledgments

The team of authors would like to thank the management of the Smolensk branch of the Saratov State Law Academy and the Bar Association «Partner» (Smolensk) for their help in organizing and conducting research and preparing the article.

References

Lewis, C. (2015). Social media: cyber trap door to Defamation – Jamaica's Defamation act. *Masaryk University Journal of Law and Technology, 9*(1), 65–84.

Li, X., & Qin, Y. (2018). Research on Computer Network Defamation Crime in China. *Procedia Computer Science, 131,* 1217–1222.

Metchik, E. (1997). A typology of crime on the Internet. *Security Journal, 9*(1-3), 27–31.

Pastukhov, P. S. (2019). "Electronic evidence" in the regulatory system of criminal procedural evidence. *Perm legal almanak*, *2*, 692–707.

Shirkin, A. A., & Erashova, O. S. (2019). *Committing an act implying defamation on the Internet. Problems of proving and calculating the statute of limitations*. https://cyberleninka.ru/article/n/sovershenie-deyaniya-podrazumevayuschego-klevetu-v-seti-internet-problemy-dokazyvaniya-i-ischisleniya-sroka-davnosti

Shukan, A., Abdizhami, A., Ospanova, G., & Abdakimova D. (2019). Crime control in the sphere of information technologies of Turkey. *Digital Investigation*, *30*, 94–100.

Vekhov, V. B. (2016). Electronic evidence: problems of theory and practice. *Law and order: history, theory, practice, 4*(11), 46–50.